# ABSTRACT

A public-key encryption scheme provides a provable security against adaptive-chosen-ciphertext-attacks (ACCA) and reduces the length of a ciphertext in a public-key encryption system. For the above purposes, the public-key encryption scheme is based on a weaker assumption, a computational Diffie-Hellman assumption (CDH-A) than a fundamental assumption, a decisional Diffie-Hellman assumption (DDH-A) and analyzes the security of the ciphertext in a random oracle model. Thus, the method guarantees provable security and length-efficiency.